REMARKS

Claims 1-8 have been examined with all claims rejected based on prior art. More specifically, claims 1-5 and 8 have been rejected under 35 USC 102(e) as being anticipated by Kash et al. (U.S. Patent No. 6,515,304; hereinafter "Kash"), and claims 6 and 7 have been rejected under 35 USC 103(a) as being unpatentable over Kash in view of Klughart et al. (U.S. Patent No. 6,396,137; hereinafter "Klughart"). Applicant respectfully traverses this rejection for the reasons set forth below.

The invention is concerned with techniques of preventing unauthorized external access to operation of integrated digital circuits, and particularly with countermeasures against so-called side-channel attacks which are performed by unauthorized parties for analyzing integrated digital circuits, for example, for analyzing coding algorithms performed by microprocessors.

Typically, integrated circuits are so-called synchronous circuits which operate on the basis of a clock signal.

It is a standard approach in the prior art to introduce random wait states into the operation of such synchronous circuits to thus randomly delay the time of operation of such synchronous circuits, i.e. when such synchronous circuits carry out internal algorithms. In a typical approach, an external clock is internally randomly delayed within the synchronous circuit to thus randomly postpone the occurrence of internal operations, like the operation of internal coding algorithms.

The subject matter of the independent claims establishes a high security against attacks by unauthorized persons trying to analyze internal operations, like coding algorithms, by combining two measures, namely:

- the use of digital circuits which are implemented as <u>asynchronous circuits</u>; and

- the time varying of the supply voltage of the asynchronous circuit to thereby time-shift the execution of the time of operations within said asynchronous circuit.

The applied prior art does not add anything to the prior art as discussed above. To be more specific, in connection with Fig. 6, Kash discloses a synchronous circuit having an external clock reference, an on-chip phase lock loop and a clock signal conditioning circuit receiving an output signal from the external clock reference in order to establish a phase lock loop clock signal on the chip, a subsequent random delay generator for introducing a jitter into the clock signal, and an internal circuitry receiving the jittered clock. Kash is merely an example of the above-discussed prior art synchronous circuits having a random generator for introducing random wait states into the process flow or variations into the clock.

Therefore, Kash is silent about the provision of asynchronous circuits which, by definition, are self-timed circuits. It is a characteristic of asynchronous circuits that their processing is not related to any time-periodic events, such as a clock.

Furthermore, Kash does not suggest varying the supply voltage of an asynchronous circuit. Rather, in the Fig. 6 embodiment, a random delay is introduced into the clock of the synchronous circuit.

The Examiner further refers to column 3, line 51, through column 4, line 3 of Kash. This section of Kash does not refer to the variation of a supply voltage. Rather, it refers to a time-varying voltage across an interface which produces a time-varying modulation of the reflectivity from the interface (see column 3, line 66, through column 4, line 2).

Klughart deals with additional security to provide an integrated circuit from reverse engineering efforts by third parties (see column 34, lines 42 through 48). However, Klughart neither suggests making use of asynchronous circuits nor does it contain any teaching to vary the supply voltage of such asynchronous circuits. Rather, Klughart teaches covering regulators and switches in integrated circuits with separate sets of metal and semiconductor layers in order to prevent unauthorized access (see column 34, lines 49-64).

Thus, claims 1-8, along with new dependent claims 9 and 10, are patentable over the applied references for at least these reason.

In view of the above, Applicant believes the pending application is in condition for allowance.

In the event a fee is required or if any additional fee during the prosecution of this application is not paid, the Patent Office is authorized to charge the underpayment to Deposit Account No. 50-2215.

Dated: May 17, 2007

Respectfully submitted,

By Laura C. Brutman
Laura C. Brutman
Registration No.: 38,395
DICKSTEIN SHAPIRO LLP
1177 Avenue of the Americas
41st Floor
New York, New York 10036-2714
(212) 277-6500
Attorney for Applicant